LISTING OF CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method for controlling a ~~the~~ disclosure time of information by a publisher to one or more recipients comprising:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

the trusted body providing a digital certificate signed with a private key of the trusted body to the publisher prior to the specified date and time, the digital certificate providing the publisher with the encryption key prior to the specified date and time;

the publisher using the encryption key to encrypt data;

the recipient obtaining the encrypted data; and

the trusted body making the decryption key available to the recipient at the specified date and time, wherein the trusted body generates one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers, and each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

2. (Currently amended) The method of ~~A method as claimed in~~ claim 1, wherein the publisher verifies the signature on the digital certificate with the public key of the trusted body.

3. (Currently amended) The method of ~~A method as claimed in~~ claim 1, wherein the encryption key is a public key and the decryption key is another private key in a public key infrastructure.

4. (Currently amended) The method of ~~A method as claimed in~~ claim 1, wherein the trusted body creates the ~~an~~ asymmetrical key pair for the ~~a~~ specified date and time on demand from the ~~a~~ publisher.

5. (Currently amended) The method of ~~A method as claimed in~~ claim 1, wherein the trusted body generates one key pair for the ~~a~~ specified date and time.

6. (Cancelled)

7. (Cancelled)

8. (Currently amended) The method of ~~A method as claimed in~~ claim 1, wherein the decryption key is encrypted with a public key and only recipients with the corresponding private key can obtain the decryption key.

9. (Currently amended) A system for controlling a ~~the~~ disclosure time of information comprising:

a publisher;

a trusted body;

an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

a digital certificate signed with a private key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time; and

means for making the decryption key available at the specified date and time, wherein there is a plurality of publishers, one or more asymmetrical key pairs for the specified date and time, a different asymmetrical key pair for each of the plurality of publishers, and each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

10. (Currently amended) The system of ~~A system as claimed in~~ claim 9, including one or more recipients with means for obtaining data encrypted with the encryption key from the publisher prior to the specified date and time and means for obtaining the decryption key at or after the specified date and time.

11. (Currently amended) The system of ~~A system as claimed in~~ claim 9, wherein the certificate includes the specified date and time, the encryption key ~~value~~, and a ~~the~~ name of the trusted body.

12. (Currently amended) The system of ~~A system as claimed in~~ claim 9, wherein the encryption key is a public key and the decryption key is another private key in a public key infrastructure.

13-15. (Cancelled)

16. (Currently amended) The system of ~~A system as claimed in~~ claim 9, wherein the decryption key is encrypted with a public key and only recipients with a ~~the~~ corresponding private key can obtain the decryption key.

17. (Currently amended) The system of ~~A system as claimed in~~ claim 9, wherein the trusted body has one or more agents who act on behalf of the trusted body.

18. (Currently amended) The system of ~~A system as claimed in~~ claim ~~17~~ 9, wherein an agent for the trusted body is a smart card having an internal clock for providing the decryption key to a recipient.

19. (Currently amended) The system of ~~A system as claimed in~~ claim 10, wherein the trusted body is accessible by the publisher and the recipients via a communication network.

20. (Currently amended) A method for controlling a ~~the~~ disclosure time of information by a publisher to one or more recipients comprising:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

the trusted body providing the publisher with the encryption key prior to the specified date and time;

the publisher using the encryption key to encrypt data;

the recipient obtaining the encrypted data; and

the trusted body making the decryption key available to the recipient at the specified date and time;

wherein the trusted body generates one or more asymmetrical key pairs for the ~~a~~ specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers, wherein each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

21. (Cancelled)

22. (Currently amended) The method of ~~A method as claimed in~~ claim 20, wherein the decryption key is encrypted with a public key ~~ke y~~ and only the recipient[[s]] with a ~~the~~ corresponding private key can obtain the decryption key.

23. (Currently amended) A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the steps of claim 1 when said product is run on ~~a~~ the digital computer.

24. (Currently amended) An information distributing service for controlling a ~~the~~ disclosure time of information by a publisher to one or more recipients comprising:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

the trusted body providing a digital certificate signed with a private key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time;

the publisher using the encryption key to encrypt data;

the recipient obtaining the encrypted data; and

the trusted body making the decryption key available to the recipient at the specified date and time, wherein the trusted body is configured to generate one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers, and each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.